# STANDARD INTERFEJSU REJESTRÓW AKCJONARIUSZY (SIRA)

Specyfikacja interfejsu API przygotowana na potrzeby cyfrowego dostępu do elektronicznych rejestrów akcjonariuszy

Luty 2021
Wersja 1.0

## Licencja

Dokumentacja Standardu Interfejsu Rejestrów Akcjonariuszy (dalej: SIRA) jest dostępna na licencji Creative Commons[1].

## Historia wersji

| Nr wersji | Data publikacji |
|---|---|
| 1.0 | 08.02.2021 |


Bartosz Biliński, Anchor Software

dr Jakub Guzikowski, PKO Bank Polski

Janusz Łaski, ING Bank Śląski

Kruszewski Adrian, Anchor Software

Krzysztof Urbański, 7bulls

Łukasz Wiśniewski, PKO Bank Polski

Małgorzata Kalinkowska, PKO Bank Polski

Marcin Jurkowski, Santander Bank Polska

Piotr Rutkowski, KRPM/NASK

Tomasz Kalicki, Kancelaria DZP


1 https://creativecommons.org/licenses/by/3.0/pl/

# SPIS TREŚCI

# SŁOWNIK POJĘĆ

**Akcjonariusz** – oznacza akcjonariusza Emitenta.

**API** – oznacza zbiór reguł ściśle opisujący, w jaki sposób programy lub podprogramy komunikują się ze sobą (ang. Application Programming Interface).

**Aplikacja dostępowa** – aplikacja umożliwiająca dostęp do danych zawartych w Systemach poprzez API.

**Emitent** – oznacza spółkę akcyjną niebędącą spółką publiczną w rozumieniu art. 4 pkt. 10 ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych.

**KSH** – oznacza ustawę z dnia z dnia 15 września 2000 r. – Kodeks spółek handlowych.

**PPRA** – oznacza podmiot prowadzący rejestr akcjonariuszy.

**Rejestr Akcjonariuszy** – oznacza rejestr akcjonariuszy prowadzony przez podmiot prowadzący rejestr akcjonariuszy w trybie określonym art. 328(1) i n. KSH.

**SALT** - nazwa wartości, która służy do wzbogacenia techniki przechowywania haseł w sposób bezpieczny.

**Seed** – zbiór słów umożliwiający odzyskanie uprawnień w Aplikacji dostępowej.

**System** – oznacza system teleinformatyczny, prowadzony przez podmiot prowadzący rejestr akcjonariuszy udostępniany Emitentowi na podstawie umowy zawartej pomiędzy Emitentem, a PPRA, do którego Dostęp może być przyznany Akcjonariuszowi, na zasadach i w zakresie określonym szczegółowo w tej umowie.

# 1. WSTĘP

## 1.1. Kontekst

Nowelizacja Kodeksu Spółek Handlowych wprowadziła do polskiego porządku prawnego obowiązek dematerializacji akcji spółek akcyjnych i komandytowo-akcyjnych niebędących spółkami publicznymi. W praktyce oznacza to, iż akcje zapisane w formie papierowej muszą zostać zastąpione zapisem elektronicznym w odpowiednim rejestrze. W myśl art. 328 KSH rejestr może być prowadzony w formie rozproszonej i zdecentralizowanej co wskazuje na możliwość zastosowania technologii blockchain:

**„§ 3. Rejestr akcjonariuszy jest prowadzony w postaci elektronicznej, która może mieć formę rozproszonej i zdecentralizowanej bazy danych."**

W nawiązaniu do powyżej wskazanej możliwości oraz innych perspektywicznych zagadnień z obszaru R&D, na początku 2020 roku powstał zespół w ramach inicjatywy Blockchain Lab prowadzonej przez Koalicję na Rzecz Polskich Innowacji (dalej: KPI) składający się z różnych przedstawicieli szeroko rozumianego rynku finansowego (banków, startupów, kancelarii prawnych, firm technologicznych). W ramach wspólnych warsztatów rozpoczęto projekt, mający na celu wypracowanie oddolnego standardu dostępności do danych zawartych w elektronicznych rejestrach akcjonariuszy, który będzie bazował na wykorzystaniu narzędzi powszechnie stosowanych do interakcji z rozwiązaniami opartymi o technologię blockchain.

Niniejszy dokument jest efektem wielomiesięcznych prac R&D zespołu projektowego, które znacznie wykroczyły poza ramy KPI i stanowi on zarówno propozycję implementacji konkretnych rozwiązań w formule wypracowanego przez rynek nieoficjalnego standardu, jak i solidny punkt wyjścia do dalszych prac w obszarze technologii blockchain. Warto również podkreślić, iż podmioty wdrażające SIRA, które przygotowały założenia o charakterze normalizacyjnym na co dzień ze sobą konkurują. Jednakże podmioty te wykorzystały okazję do rozwoju projektu w ramach grupy roboczej ds. rejestrów rozproszonych i blockchain dzia-

łająca przy KPRM (d. ministerstwo cyfryzacji), co stanowi modelowy sposób samoorganizacji i współpracy interesariuszy rynku z państwem, w celu zapewnienia warunków dla rozwoju zastosowań technologii przełomowych, do których należy blockchain.
Dokument SIRA został opublikowany w miejscu zachowującym neutralność wobec interesariuszy rynku, czyli na stronie grupy roboczej ds. rejestrów rozproszonych i blockchain działającej w KPRM:

https://www.gov.pl/web/cyfryzacja/blockchain/SIRA

## 1.2 Struktura dokumentu

Dokument składa się z trzech podstawowych części:

| | |
|---|---|
| **Rozdział 1 - 2** | Część dotycząca wprowadzenia do zagadnień związanych z elektronicznym rejestrem akcjonariuszy i niniejszą inicjatywą |
| **Rozdział 3** | Część dotycząca proponowanych prawnych sformułowań umożliwiających przystąpienia do SIRA |
| **Rozdział 4** | Część dotycząca specyfikacji technicznej interfejsu API oraz związanych z nim procesów |

## 1.3 Misja SIRA

Podstawowym celem dokumentu jest zdefiniowanie interfejsu dostępowego do elektronicznych rejestrów akcjonariuszy. Niniejszy standard jest rozwiązaniem będącym propozycją dla wszystkich podmiotów uprawnionych do prowadzenia elektronicznych rejestrów akcjonariuszy (dalej: PPRA), oraz dostawców aplikacji, którzy chcą wyświetlać na rzecz swoich klientów dane o ich aktywach zapisane w rejestrach akcjonariuszy. Wierzymy, iż wymóg zniesienia formy materialnej akcji (potocznie zwany również dematerializacją) jest nie tylko obowiązkiem, ale również szansą dla spółek nim objętych do skorzystania z szerokiej gamy możliwości oferowanych przez nowe technologie, w tym w szczególności technologię blockchain.

Opisane w pierwszej wersji standardu funkcjonalności stanowią realną wartość dla akcjonariuszy w postaci szerszego i możliwie wygodnego wglądu do zawartości poszczególnych rejestrów. Dodatkowo są one pierwszym wspólnym krokiem podmiotów z rynku bankowego inicjujących standard w kierunku wdrożeń o charakterze R&D w następujących obszarach:

**1.** Tokenizacja akcji oraz Złotego w celu m.in. rozliczeń w modelu „Atomic Swap" oraz automatycznej wypłaty pożytków (dywidend) na bazie smart kontraktów;
**2.** Zdecentralizowany obrót wtórny (bez obrotu zorganizowanego);
**3.** Wykorzystanie suwerennej cyfrowej tożsamości, korzystającej z rozmaitych dostawców usług zaufania.

## 1.4. Status prawny dokumentu

Niniejszy dokument nie ma charakteru wiążącego dla podmiotów będących sygnatariuszami SIRA lub podmiotów, które przestrzegają zawartych w dokumencie zaleceń i postanowień. Wszelkie propozycje mają charakter dobrowolnego zastosowania, a podmioty, które dostosują się do zapisów niniejszego dokumentu w każdym momencie mają prawo do zaprzestania czynności, które w związku z SIRA podjęły. Odstąpienie nie rodzi żadnych konsekwencji.

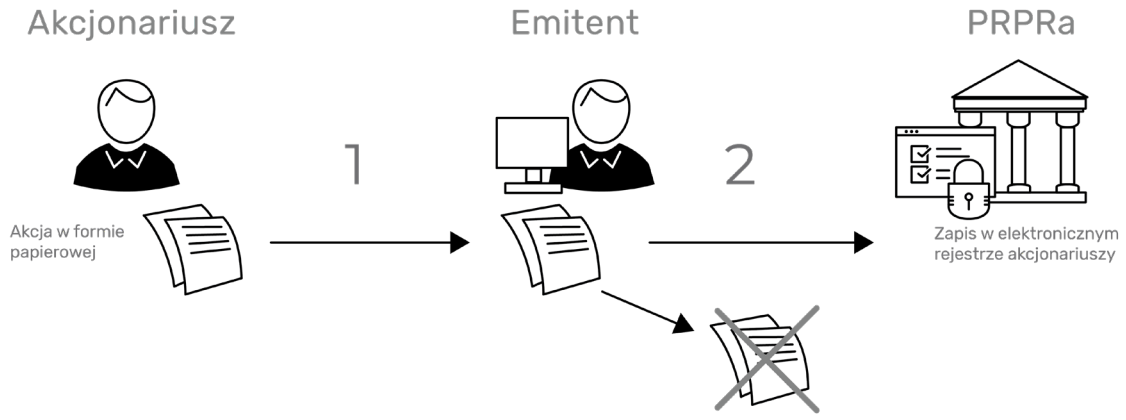
SIRA dotyczy wybranych kwestii technicznych związanych z dostępem do rejestru akcjonariuszy wyraźnie w niniejszym dokumencie wskazanych, a w szczególności nie obejmuje kwestii związanych z ochroną danych osobowych i przekazywaniem danych klientów, przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, usługami płatniczymi ani obrotem papierami wartościowymi i instrumentami finansowymi.

Standard ma charakter ogólny i jego przyjęcie nie zwalnia od adekwatnej oceny prawnej i technicznej zaproponowanych rozwiązań przez podmioty go stosujące.

# 2. ELEKTRONICZNY REJESTR AKCJONARIUSZY

## 2.1 Proces zniesienia formy dokumentowej akcji

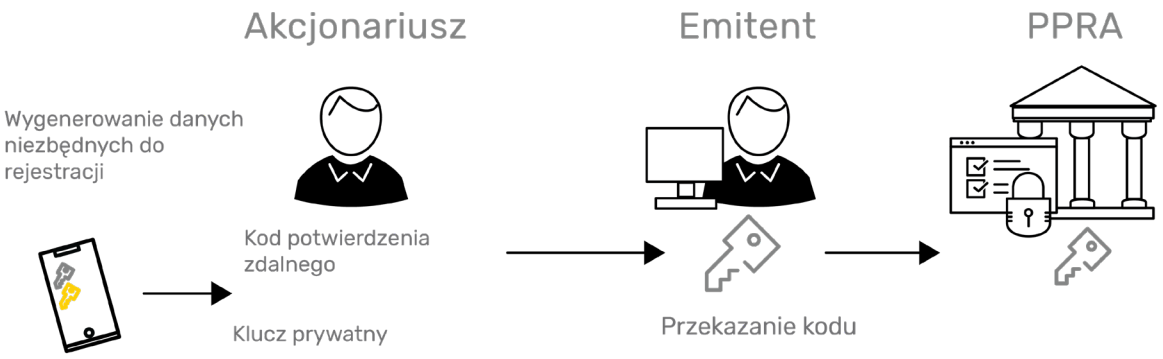
W okresie do 1 marca 2021 roku nienotowane spółki akcyjne oraz spółki komandytowo-akcyjne (dalej: emitenci) mają obowiązek co najmniej 5-krotnego wezwania swoich akcjonariuszy w celu zarejestrowania i zdeponowania posiadanych w postaci materialnej papierów wartościowych.
Oznacza to, iż akcjonariusz posiadający np. akcje na okaziciela w formie dokumentu papierowego powinien stawić się w miejscu wyznaczonym przez danego emitenta, przekazać dokumenty akcji oraz podać wszelkie niezbędne dane dodatkowe (m.in. imię, nazwisko/firmę, adres). Po poprawnym przejściu całego procesu akcjonariusz otrzyma potwierdzenie przyjęcia akcji, które do dnia 1 marca 2021 roku będzie stanowiło dowód, iż jest on właścicielem przekazanych papierów wartościowych. Począwszy od wskazanego dnia akcją właściwą będzie akcja widniejąca w elektronicznym rejestrze akcjonariuszy. Warto również dodać, iż elektroniczne rejestry akcjonariuszy nie mogą być prowadzone bezpośrednio przez emitentów. Uprawnione są do tego m.in. biura maklerskie i banki powiernicze. W konsekwencji, emitenci muszą przekazać zebrane dane o swoich akcjonariuszach w celu zainicjowania rejestrów elektronicznych.



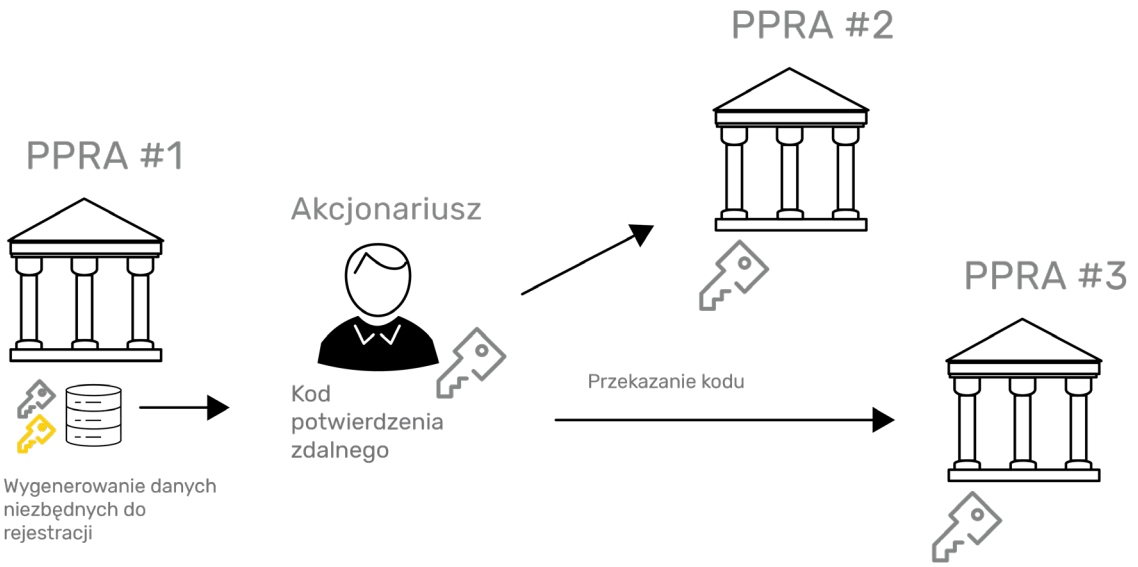
## 2.2 Dodatkowy element procesu

W ramach możliwości, które stwarza SIRA proponujemy, aby w procesie kontaktu z akcjonariuszami emitenci zbierali również kod potwierdzenia zdalnego (swojego rodzaju login, inaczej tzw. adres) powiązany matematyczną zależnością z kluczem prywatnym (swojego rodzaju hasło), który posiada jedynie akcjonariusz deponujący akcje. Rejestracja kodu umożliwi przede wszystkim zdalny dostęp do danych z elektronicznych rejestrów akcjonariuszy w ramach bezpośredniego kontaktu akcjonariusza z PPRA.

Sposób wygenerowania kodu opisano szczegółowo w punkcie 4.1. W tym momencie warto jednak zaznaczyć, iż akcjonariusz może we własnym zakresie wygenerować poprawny kod i powiązany z nim klucz prywatny. W celu wygenerowania takiego zestawu nie wymagana jest interakcja z emitentem lub PPRA, ale wskazane jest skorzystanie z aplikacji, która w późniejszym okresie umożliwi automatyczne pobieranie danych i interakcje z systemami PPRA.



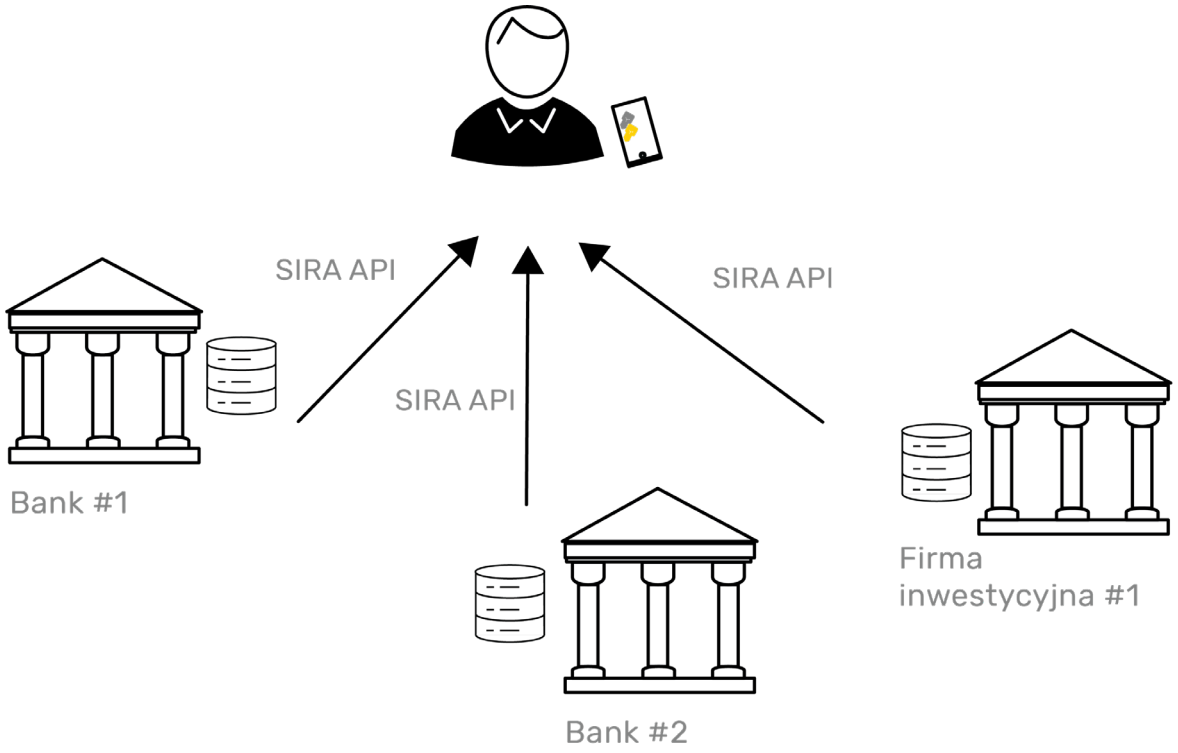

Akcjonariusze, którzy nie zarejestrują swoich kodów w procesie dematerializacji będą mogli zarejestrować kod bezpośrednio w aplikacjach podmiotów prowadzących rejestry akcjonariuszy. W niektórych przypadkach możliwe będzie również wygenerowanie zestawu danych uwierzytelniających bezpośrednio w aplikacji PPRA.




## 2.3 Uzasadnienie wybranego rozwiązania

Warto podkreślić dlaczego opisany proces rejestracji klucza przeważa nad innymi rozwiązaniami w tym obszarze. Po pierwsze, raz wygenerowany zestaw kluczy może zostać zarejestrowany przez wielu emitentów i tym samym stanowić dostęp do wielu baz danych podmiotów prowadzących rejestry. Zatem ten sam akcjonariusz nie musi wyrabiać kilku kont w różnych aplikacjach PPRA, a będzie miał możliwość wyświetlenia **wszystkich swoich aktywów objętych dematerializacją w jednym miejscu.**

Po drugie, specyfikację kluczy publicznych dotyczących danego standardu wybrano nieprzypadkowo. Tak przygotowywany zestaw do uwierzytelnienia potencjalnie może w przyszłości służyć również do zarządzania stokenizowanymi akcjami oraz innymi cyfrowymi aktywami w postaci tokenów osadzonych w sieciach blockchain, przełożyć się na obsługę tzw. smart kontraktów lub inne czynności definiowane przez KSH (np. wypłata dywidendy lub wystawienie świadectwa rejestrowego).




Pomijając kwestie doinformowania akcjonariusza oraz sposobu przekazania klucza, które poszczególne implementacje standardu będą rozwiązywały na swój sposób, opisane rozwiązanie wydaje się racjonalnym wyborem dla wszystkich akcjonariuszy posiadających akcje zarejestrowane w kilku podmiotach prowadzących rejestry akcjonariuszy.

## 2.4 Prosta spółka akcyjna

SIRA potencjalnie obejmuje swoimi możliwościami również rejestry prostych spółek akcyjnych, które od samego początku będą prowadzone w postaci elektronicznej. Jednakże zapisy pierwszej wersji publikacji dotyczą wyłącznie rejestrów spółek akcyjnych i komandytowo-akcyjnych podlegających obowiązkowej dematerializacji. Niemniej jednak intencją autorów jest dalsze wspólne prowadzenie prac o charakterze R&D i rozszerzenie inicjatywy SIRA o analizy i ustalenia dotyczące prostych spółek akcyjnych.

# 3. ZAGADNIENIA PRAWNE

Zaleca się, aby podmioty, które przystąpią do inicjatywy SIRA odpowiednio zmodyfikowały zapisy regulaminów swoich aplikacji służących do prowadzenia i udostępniania elektronicznych rejestrów akcjonariuszy.

Wychodząc naprzeciw konieczności zmiany zapisów, autorzy SIRA wypracowali propozycję zestawu definicji pojęć oraz poszczególnych zapisów, którymi mogą posłużyć się PPRA. Należy podkreślić, iż poniższe definicje i poszczególne zapisy mają charakter przykładowy i ich szczegółowe brzmienie może być odmienne w regulaminach różnych instytucji.

## 3.1 Propozycja zapisów uzupełniających słownik pojęć

**Akcjonariusz [**lub: **Użytkownik] -** oznacza akcjonariusza Emitenta.

**API** – oznacza zbiór reguł ściśle opisujący, w jaki sposób programy lub podprogramy komunikują się ze sobą (ang. *Application Programming Interface*).

**Dostęp** – oznacza uzyskanie dostępu przez [Akcjonariusza] do informacji i danych bezpośrednio go dotyczących zawartych w Rejestrze Akcjonariuszy.

**Emitent [**lub: **Spółka / Klient]** – oznacza spółkę akcyjną niebędącą spółką publiczną w rozumieniu art. 4 pkt. 10 ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizo-

wanego systemu obrotu oraz o spółkach publicznych.

**KSH** – oznacza ustawę z dnia z dnia 15 września 2000 r. – Kodeks Spółek Handlowych.

**Podmiot Prowadzący Rejestr Akcjonariuszy [lub: PPRA/ Dom Maklerski/Bank]** – oznacza podmiot prowadzący Rejestr Akcjonariuszy.

**Rejestr Akcjonariuszy** – oznacza rejestr akcjonariuszy prowadzony przez Podmiot Prowadzący Rejestr Akcjonariuszy w trybie określonym art. 328(1) i n. KSH.

**Standard** – oznacza dokumentację Standardu Interfejsu Rejestrów Akcjonariuszy opublikowaną pod adresem https://www.gov.pl/web/cyfryzacja/blockchain/SIRA

**System** – oznacza system teleinformatyczny, prowadzony przez Podmiot Prowadzący Rejestr Akcjonariuszy udostępniany Emitentowi na podstawie Umowy, do którego Dostęp może być przyznany Akcjonariuszowi,na zasadach i w zakresie określonym szczegółowo w Umowie.

**Uwierzytelnienie** – oznacza potwierdzenie (identyfikację), że użytkownik jest tym, za kogo się podaje, w sposób szczegółowo opisany w standardzie.

# 3.2 Propozycja zapisów uzupełniających treść regulaminu

§ [•]. Uwierzytelnienie

1. Uwierzytelnienie Akcjonariusza dla celów Dostępu do Rejestru Akcjonariuszy dokonywane jest za pomocą pary kryptograficznych kluczy asymetrycznych, tj. klucza prywatnego i klucza publicznego oraz pochodnych im danych. Oba klucze generowane są przez Akcjonariusza zgodnie ze Standardem, przy czym:

a) klucz prywatny Akcjonariusz pozostawia wyłącznie dla swojej wiadomości
b) klucz publiczny Akcjonariusz przekazuje Emitentowi i/lub Podmiotowi Prowadzącemu Rejestr Akcjonariuszy

2. Akcjonariusz podpisuje wnioski / dyspozycje składane przez siebie w Systemie przy użyciu swojego klucza prywatnego. Podmiot Prowadzący Rejestr Akcjonariuszy przy pomocy uprzednio zarejestrowanego klucza publicznego lub danych mu pochodnych sprawdza prawidłowość podpisu Akcjonariusza.

3. Sposób generowania pary kryptograficznych kluczy asymetrycznych zostanie przekazany do wiadomości Akcjonariuszy, w szczególności w drodze wiadomości elektronicznej przesłanej na adres wskazany przez Akcjonariusza lub w inny sposób rekomendowany w Standardzie.

4. Szczegółowy opis rozwiązań technologicznych oraz danych służących do przeprowadzenia ww. identyfikacji (uwierzytelnienia) Akcjonariusza w Systemie, w tym standardu technicznego generowania kluczy oraz sposobu podpisywania przy ich pomocy wniosków i dyspozycji składanych w Systemie jest zgodny ze Standardem dostępnym pod adresem:
https://www.gov.pl/web/cyfryzacja/blockchain/SIRA

# 4. ZAGADNIENIA TECHNICZNE

## 4.1 Standard kluczy kryptograficznych

Dla przyjęcia jednolitego standardu generowania kluczy na potrzeby rejestrów akcjonariuszy proponuje się wykorzystanie standardu stosowanego do generowania kont w sieci Ethereum. Procedura generowania takiego klucza składa się z następujących kroków:

1. Generowany jest losowy klucz prywatny o długości 32 bajtów (64 znaków z zapisie heksadecymalnym)

2. Następnie na podstawie tak wylosowanego klucza prywatnego generowany jest klucz publiczny z wykorzystaniem algorytmu ECDSA (Elliptic Curve Digital Signature Algorithm), w tym konkretnym przypadku z zastosowaniem algorytmu secp256k1
https://www.gov.pl/web/cyfryzacja/blockchain/SIRA

3. Następnie generowany jest publiczny adres Ethereum (kod potwierdzenia zdalnego) poprzez przetworzenie klucza publicznego z wykorzystaniem funkcji mieszającej keccak256 i wykorzystaniu najbardziej znaczących 20 bajtów (znaków w zapisie heksadecymalnym).

Wizualizacja powyższego procesu:
https://www.royalfork.org/2017/12/10/eth-graphical-address/

Nie zalecane jest korzystanie z powyższej strony w celu wygenerowania kodu potwierdzenia zdalnego / adresu.

## 4.2 Lista punktów dostępowych API

| Punkt dostępowy | Zakres działania |
|---|---|
| /challenge | Metoda służąca do wygenerowania danych niezbędnych do uwierzytelnienia w ramach /login. |
| /login | Metoda służąca do uwierzytelnienia akcjonariusza w imieniu którego wysyłane będą kolejne zapytania. |
| /peers | Metoda służąca do pobrania listy adresów API, które wspierają SIRA. |
| /issuers | Metoda wydająca listę spółek, w których dany akcjonariusz posiada aktywa. |
| /myassets | Metoda wydająca szczegółowy zestaw danych o aktywach akcjonariusza, który uzupełnia informacje z /issuers. |
| /registry | Metoda wydająca rejestr akcjonariuszy. |
| /shareholders | Metoda wydająca dane o akcjonariuszu. |

### 4.2.1 Punkt dostępowy **/challenge**

W ramach /challenge Aplikacja dostępowa powinna przekazać PPRA tzw. adres będący pochodną klucza publicznego zarejestrowanego przez akcjonariusza. Informacje na temat sposobu tworzenia adresu zawarto w 4.1. PPRA po weryfikacji czy dany adres był uprzednio zarejestrowany przesyła w odpowiedzi dane, które są niezbędne do uwierzytelnienia metodą /login.
Aplikacje w celu skutecznej interakcji z punktem dostępowym /challenge muszą wykorzystać niekwalifikowany certyfikat infrastruktury typu Standard Server przydzielany przez Krajową Izbę Rozliczeniową. Certyfikat zostanie wystawiony dla kluczy RSA/ECC wygenerowanych samodzielnie przez użytkownika. Certyfikat można uzyskać w procesie całkowicie zdalnym.

### 4.2.2 Punkt dostępowy **/login**

W ramach /login Aplikacja dostępowa powinna przekazać PPRA dane otrzymane w ramach /challenge podpisane kluczem prywatnym powiązanym kryptograficznie uprzednio zarejestrowanym adresem (kod potwierdzenia zdalnego). PPRA po weryfikacji tego czy dany adres był uprzednio zarejestrowany, odsyła token zaszyfrowany na klucz publiczny powiązany z otrzymanym adresem. Token uprawnia aplikację dostępową do korzystania z pozostałych punktów dostępowych.

### 4.2.3 Punkt dostępowy **/peers**

Punkt dostępowy /peers ma za zadanie udostępnić listę adresów API poszczególnych PPRA. Jego powstanie jest bezpośrednią odpowiedzią na ryzyko tego, iż centralna instytucja utrzymująca taką listę przestanie wspierać inicjatywę SIRA. Aplikacja dostępowa, która chce korzystać z SIRA powinna znać przynajmniej jeden adres API PPRA, który udostępnia punkt dostępowy typu /peers. Lista adresów API podmiotów inicjujących SIRA zamieszczona została poniżej:

ING Bank Śląski: TBD
PKO Bank Polski: sira.pkobp.pl
Santander Bank Polska: www.santander.pl/sira

Punkt dostępowy /peers w odpowiedzi zwraca listę podmiotów, które uczestniczą w SIRA. Lista składa się z dwóch części zawierających odpowiednio informację na temat lokalizacji aktywnych i wycofanych API.

## Wpis na listę aktywnych API

PPRA, które chce dołączyć do niniejszej inicjatywy powinno zgłosić się do jednego z już zaangażowanych PPRA, które podtrzymuje w swoim API punkt dostępowy /peers.

Dodanie nowego uczestnika SIRA wykonuje ręcznie administrator systemu danego PPRA poprzez dopisanie do listy nowego adresu. PPRA powinny cyklicznie w ustalonych we własnym zakresie odstępach czasu (np. raz dziennie) odpytywać pozostałe PPRA i uzupełniać własne listy wystawiane w ramach /peers.

## Wykreślenie z listy aktywnych API / Wpis na listę wycofanych API

Proces wykreślenia z listy aktywnych API działa analogicznie do wpisu. Dowolne z PPRA biorących udział w zdecentralizowanej wymianie listy może zaproponować wykreślenie konkretnego adresu z listy. Do decyzji i ręcznej zmiany administratorów API poszczególnych PPRA pozostaje czynność przeniesienia danej lokalizacji API z aktywnych do wykreślonych.

### 4.2.3 Punkt dostępowy **/issuers**

Punkt dostępowy /issuers umożliwia otrzymanie kompletnej listy spółek w postaci numerów KRS, w której dany akcjonariusz posiada papiery wartościowe. Otrzymane numery KRS służą do generowania kolejnych bardziej szczegółowych zapytań.
Opcjonalna część odpowiedzi /issuers została zaprojektowana z myślą o aplikacjach mobilnych, które w pierwszej kolejności wyświetlą nazwy dostępnych spółek wraz z prostymi podsumowanymi informacjami na ich temat.

PPRA, które chcą wystawić /issuer w odpowiedzi powinny dostarczyć co najmniej następujące dane na temat:

A) **issuer_name** - nazwy spółki
B) **issuer_krs_number** - numeru KRS spółki

Opcjonalnie wystawione mogą być dane dotyczące:

C) **issuer_address** - adresu spółki
D) **issuer_registration_date** - daty zarejestrowania spółki
E) **issuer_NIP** - numeru NIP spółki
F) **issuer_regon** - numeru REGON spółki
G) **number_of_my_assets** - liczby papierów wartościowych
H) **my_share_in_equity** - udziału w kapitale

Informacje dotyczące zaangażowania akcjonariusza:
**G-H** dotyczą zaangażowania w daną spółkę akcjonariusza w imieniu którego przesłane jest zapytanie.

## 4.2.4 Punkt dostępowy **/myassets**

Zadaniem punktu dostępowego /myassets jest przekazanie danych o aktywach akcjonariusza w imieniu, którego odpytywane jest API. PPRA, które chcą wystawić /myassets w odpowiedzi powinny dostarczyć co najmniej następujące dane na temat:

A) **emission_date** - daty emisji danej serii akcji
B) **series** - oznaczenia serii
C) **paper_number_from** - początku zakresu akcji
D) **paper_number_to** - końca zakresu akcji
E) **isin** - oznaczenia serii typu ISIN
F) **paper_ISIN_number** - liczby akcji dla oznaczenia ISIN
G) **nominal_value** - wartości nominalnej akcji
H) **is_paid** - potwierdzenia opłacenia (0-1)

Opcjonalnie wystawione mogą być dane dotyczące:

I) **paper_type** - daty emisji danej serii akcji
J) **limitations** - oznaczenia serii
K) **special_authorizations** - początku zakresu akcji
L) **addnotations** - końca zakresu akcji

### Zakres akcji:

**C-D** – z uwagi na to, iż w dosyć często elektroniczne rejestry akcjonariuszy zawierają wpisy, które pomiędzy sobą różnią się jedynie numerem akcji, w ramach odpowiedzi zarówno /myassets, jak i /registry zdecydowano się agregować takie wpisy do zakresów. Zakres definiowany jest przez numer akcji rozpoczynającej i kończącej serię jednolitych wpisów.
W skrajnym przypadku zakres może dotyczyć jednej akcji
(np. paper_number_from: 154, paper_number_to: 154).

### Zakres akcji vs ISIN

**C-F** – w niektórych rejestrach akcjonariuszy mogą wystąpić papiery wartościowe oznaczone kodem ISIN dla których nie istnieją pojedyncze numery akcji, a jedynie ich liczba. Zatem w odpowiedzi zarówno /myassets, jak i /registry pojawią się serie akcji oraz ich zakresu i/lub kody ISIN oraz przypisane im liczby akcji. PPRA lub Aplikacje dostępowe, które podają wyświetlają liczbę akcji dla aktywów oznaczonych serią mogą wyliczyć tę wartość na podstawie udostępnianych w zakresów.

### Ograniczenia / uprawnienia szczególne / potwierdzenie opłacenia

**H,J,K,L** – dane dotyczące ograniczeń **(J)** i uprawnień szczególnych nałożonych na poszczególne akcje **(K)** oraz potwierdzenie, iż dane akcje zostały pokryte w pełnej wartości kwoty nominalnej **(H)** /myassets i /registry zwraca w na zasadzie odpowiedzi prawda/fałsz.

W ramach pola „addnotations" **(L)** PPRA mają możliwość uzupełnić tę informację o szczegóły danych uprawnień, ograniczeń lub o stopień pokrycia akcji.

## 4.2.4 Punkt dostępowy **/registry**

Punkt dostępowy /registry w odróżnieniu od /myassets umożliwia otrzymanie wszystkich danych dostępnych w rejestrze akcjonariuszy. Zakres danych zawartych w rejestrze akcjonariuszy definiuje KSH. Warto podkreślić, iż dane przekazane w odpowiedzi będą dotyczyły nie tylko osoby w imieniu której przesłane zostało zapytanie, ale również wszystkich pozostałych akcjonariuszy danej spółki. PPRA, które zdecydują się wystawić /registry w odpowiedzi powinny dostarczyć co najmniej następujące dane na temat:

**Emitenta**:

A) **issuer_name** - nazwy spółki danego emitenta
B) **issuer_registration_date** - daty zarejestrowania spółki
C) **issuer_address** - adresu spółki danego emitenta

**Akcjonariusza**:

D) **owner_company** - nazwy spółki posiadającej akcje
E) **owner_name** - imienia akcjonariusza
F) **owner_surname** - nazwiska akcjonariusza

**Aktywów:**

G) **paper_type** - rodzaju papierów wartościowych
H) **emission_date** - daty emisji danej serii akcji
I) **series** - oznaczenia serii
J) **paper_number_from** - początku zakresu akcji
K) **paper_number_to** - końca zakresu akcji
L) **isin** - oznaczenia serii typu ISIN
M) **paper_ISIN_number** - liczby akcji dla oznaczenia ISIN
N) **nominal_value** - wartości nominalnej akcji
O) **is_paid** - potwierdzenia opłacenia (0-1)
P) **limitations** - ograniczeń (0-1)
Q) **special_authorizations** - uprawnień szczególnych (0-1)

Opcjonalnie wystawione mogą być dane dotyczące:

R) **owner_email** - adresu e-mail akcjonariusza
S) **addnotations** - informacji uzupełniających

### 4.2.4 Punkt dostępowy **/shareholder**

Punkt dostępowy shareholder jest niejako uzupełnieniem danych otrzymywanych z /myassets, ponieważ umożliwia pozyskanie danych dotyczących osoby odpytującej.

## 4.3. Minimalny zakres zaangażowania PPRA

Zaleca się, aby PPRA, które chcą przystąpić do niniejszej inicjatywy, w ramach interfejsu API udostępniły co najmniej metody: /challenge, /login, /issuers, /peers i /myassets. Wskazane metody stanowią minimalny zakres funkcjonalności, który prowadzi udostępniania informacji o aktywach danego akcjonariusza.

## 4.4 Aplikacje dostępowe – dobre praktyki

Aplikacje umożliwiające dostęp do danych zawartych w rejestrach akcjonariuszy powinny być możliwie użyteczne i łatwe w obsłudze dla ich użytkowników. Podmiot odpowiedzialny za przygotowanie aplikacji dostępowej powinien zadbać o zabezpieczenia uniemożliwiające nieautoryzowane pobieranie danych. W związku z powyższym, zaleca się, aby podmioty odpowiedzialne za przygotowanie aplikacji dostępowych zastosowały się do poniższych dobrych praktyk:

**1.** Aplikacje dostępowe powinny umożliwiać proste przekazanie kodu potwierdzenia zdalnego (np. skan kodu QR, przeklejenie, przesłanie ciągu znaków);

**2.** Aplikacje dostępowe powinny wyświetlać dane z rejestru w sposób przystępny dla użytkownika;

**3.** Aplikacje dostępowe powinny zostać zabezpieczone hasłem lub kodem PIN ustawionym przez użytkownika lub inną metodą uwierzytelnienia (np. skan odcisku palca, face ID, PIN);

**4.** Jeżeli aplikacja dostępowa zabezpieczona jest hasłem powinien istnieć proces identyfikujący i uniemożliwiający ustawienie słabego hasła (zbyt krótkie lub zbyt proste);

**5.** Powinien istnieć proces umożliwiający użytkownikowi aplikacji reset hasła chroniącego dostęp do aplikacji lub innej metody uwierzytelnienia;

**6.** Powinien istnieć proces umożliwiający przeniesienie uprawnień do innej aplikacji dostępowej (np. przekazanie zabezpieczenia Seed lub klucza prywatnego);

**7.** Wgląd do klucza prywatnego lub zabezpieczenia typu Seed powinien być chroniony hasłem ustawionym przez użytkownika lub inną metodą autoryzacji;

**8.** Klucz prywatny lub seed powinien być przechowywany w aplikacji w postaci zaszyfrowanej;

**9.** Sugerowane algorytmy do przechowywania klucza prywatnego lub Seed to bcrypt lub rozwiązania bazujące na PBKDF 2;

**10.** Zalecane jest zastosowanie rozwiązań typu Android keystore system /keychain;

**11.** Wszelkie hasła do których zastosowano kryptografię powinny być przechowywane z kryptograficznie wygenerowa-

ną losową SALT;

**12.** Zaleca się wykorzystanie biblioteki OpenSSL[1];

**13.** Implementacje algorytmów pseudolosowości powinny przejść testy statystycznej losowości. Zwykle algorytmy te oznaczone są przedrostkiem "secure" lub "s" np. srand (c++), SecureRandom (Java), itp.

Powyższe zalecenia dotyczą w głównej mierze mobilnych aplikacji dostępowych, ponieważ autorzy SIRA założyli, iż właśnie tego typu aplikacje będą najczęściej służyły do interakcji z rejestrami akcjonariuszy. W pozostałych kwestiach nieporuszanych powyżej zaleca się zastosowanie do aktualnej wersji standardu ASVS[2] (ang. Application Security Verification Standard).

## 4.5 Wymagania dotyczące aplikacji webowych PPRA

Z uwagi na fakt, iż dematerializacja papierów wartościowych w znacznej mierze zostanie przeprowadzona w relatywnie krótkim czasie, PPRA które planują przestrzegać postanowień niniejszego standardu powinny udostępnić możliwość rejestracji kodów potwierdzenia zdalnego również po 1 marca 2021 roku. Zaleca się umożliwienie rejestracji, zmiany lub usunięcia kodów w aplikacji prowadzonej bezpośrednio przez PPRA (o ile PPRA prowadzi taką aplikację) lub udostępnienie innego procesu spełniającego te same funkcje.

Dodatkowo wskazane jest, aby aplikacje PPRA docelowo umożliwiły również przeglądanie zarejestrowanych kluczy publicznych oraz wycofanie uprzednio zarejestrowanych kluczy publicznych.

1 https://www.openssl.org/

2 https://owasp.org/www-project-application-security-verification-standard/